PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 15.12.1999

617

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

4

Hakija Applicant	**Sonera Oy** **Helsinki**
Patenttihakemus nro Patent application no	**982728**
Tekemispäivä Filing date	**16.12.1998**
Kansainvälinen luokka International class	**G07F**

Keksinnön nimitys
Title of invention

"Menetelmä ja järjestelmä digitaalisen allekirjoituksen toteuttamiseksi"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

PRIORITY DOCUMENT

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A
P.O.Box 1160
FIN-00101 Helsinki, FINLAND

Puhelin: 09 6939 500
Telephone: + 358 9 6939 500

Telefax: 09 6939 5204
Telefax: + 358 9 6939 5204

MENETELMÄ JA JÄRJESTELMÄ DIGITAALISEN ALLEKIRJOITUKSEN TOTEUTTAMISEKSI

Esillä oleva keksintö liittyy tietoliikennejärjestelmiin ja digitaalisen tiedon allekirjoitus- ja salaustekniikkaan. Erityisesti keksintö liittyy uudentyyppiseen ja kehittyneeseen menetelmään ja järjestelmään, jonka avulla lomake tai muu allekirjoitettava sähköisessä muodossa oleva tieto voidaan allekirjoittaa ja varmistua allekirjoituksen ja allekirjoittajan oikeellisuudesta.

TEKNIIKAN TASO

Entuudestaan on tunnettua käyttää digitaalista matkaviestintä, kuten GSM-järjestelmän (Global System for Mobile Communications, GSM) matkaviestintä, kaupallisiin transaktioihin, kuten laskun tai maksun maksamiseen sähköisesti. Patenttijulkaisusta US 5,221,838 tunnetaan laite, jota voidaan käyttää maksamiseen. Julkaisussa on kuvattu sähköinen maksujärjestelmä, jossa maksupäätteenä käytetään langattomaan ja/tai langalliseen tiedonsiirtoon kykenevää päätelaitetta. Julkaisun mukaiseen päätelaitteeseen kuuluu kortinlukija, näppäimistö, ja viivakoodin lukija tietojen syöttämiseksi ja näyttö maksuinformaation esittämiseksi.

Patenttijulkaisusta WO 94/11849 tunnetaan menetelmä tietoliikennepalveluiden käyttämiseksi ja maksuliikenteen suorittamiseksi matkapuhelinjärjestelmällä. Julkaisussa kuvataan järjestelmä, johon kuuluu päätelaite, joka on yhteydessä televerkon kautta palveluntarjoajan keskustietokoneeseen, joka sisältää palveluntarjoajan maksujärjestelmän. Matkapuhelinverkon päätelaitteeseen eli matkaviestimeen voidaan lisätä tilaajan tunnistusyksikkö, joka käsittää tilaajatiedot tilaajan tunnistamiseksi ja teleliikenteen salaamiseksi. Tiedot voidaan lukea päätelaitteeseen käy-

tettäväksi matkaviestimissä. Esimerkkinä julkaisussa mainitaan GSM-järjestelmä, jossa käytetään SIM-korttia (Subscriber Identity Module, SIM) tilaajan tunnistusyksikkönä.

Julkaisun WO 94/11849 mukaisessa järjestelmässä matkaviestin on yhteydessä matkapuhelinverkon tukiasemaan. Julkaisun mukaan yhteys muodostetaan edelleen maksujärjestelmään ja maksettava määrä samaten kuin tilaajan tunnistamiseen tarvittava data välitetään maksujärjestelmään. Julkaisussa kuvatussa pankkipalvelussa asiakas asettaa pankin palvelukortin, joka sisältää SIM-yksikön, GSM-verkon päätelaitteeseen. Puhelinperustaisessa pankkipalvelussa päätelaite voi olla standardin mukainen GSM-matkaviestin. Julkaisussa kuvatulla menetelmällä voidaan käyttää langatonta tietoliikenneyhteyttä maksujen ja/tai laskujen tai muiden vastaavien pankkipalvelujen tai kassapalvelujen toteuttamiseen.

Ongelmana yllä mainituissa ratkaisuissa on, että niissä ei oteta kantaa maksun luotettavuuteen maksajan ja maksun saajan kannalta. Käytettäessä matkaviestintä maksamiseen on tärkeää, että sekä maksaja että maksun saaja voivat luottaa järjestelmään. Maksajan on tarkkaan tiedettävä, mistä maksaa, minkä verran maksaa, kenelle maksaa, miten maksaa jne. Maksun saajan on myös tarkkaan tiedettävä, kuka maksaa, mistä maksaa, minkä verran maksaa jne.

Kuten tiedetään, tiedon siirtäminen paikasta toiseen sähköisessä muodossa on helppoa. Sen sijaan vaikeampaa on varmistua siitä, että siirretty tieto säilyy siirron aikana muuttumattomana ja siitä, että esimerkiksi matkapuhelimen näytöllä esitetty tieto lähetetään juuri sellaisenaan ja muuttumattomana vastaanottajalle.

Entuudestaan on tunnettua käyttää tiivistettä, joka on lähetettävästä tiedosta muodostettu ja laskettu tietokenttä. Tiivisteen laskemiseen käytetään

yleensä algoritmia, joka on yksisuuntainen funktio eli tiivisteestä ei ole mahdollista selvittää sen muodostamiseen käytettyjä tietoja. Eräs käytettävä algoritmi voi olla SHA-1 (Secure Has Algorithm).

Digitaalisella allekirjoituksella, jota pidetään yleisenä vaatimustasona sähköisessä maksamisessa, varmistetaan välitettävän aineiston eheys ja lähettäjän alkuperä. Digitaalinen allekirjoitus muodostetaan salaamalla välitettävästä aineistosta laskettu tiiviste lähettäjän salaisella avaimella. Koska kukaan muu ei tunne lähettäjän salaista avainta, voi vastaanottaja purkaessaan salauksen lähettäjän julkista avainta käyttäen varmistua siitä, että aineisto on muuttumaton ja lähettäjän muodostama. Eräs esimerkki digitaalisessa allekirjoituksessa käytettävästä algoritmista on RSA-salausalgoritmi, joka on julkisen ja salaisen avaimen salausjärjestelmä ja jota käytetään myös viestien salaamiseen.

KEKSINNÖN TARKOITUS

Esillä olevan keksinnön tarkoituksena on poistaa edellä esitetyt ongelmat. Erityisesti esillä olevan keksinnön tarkoituksena on tuoda esiin uuden tyyppinen menetelmä ja järjestelmä lomakkeen tai muun vastaavan tiedon allekirjoittamiseksi matkaviestimellä. Tässä yhteydessä lomakkeella voidaan tarkoittaa monen tyyppistä ja -sisältöistä sähköisesti tulkittavissa olevaan viestiä, sanomaa tai tietorakennetta. Lomake voi olla olio- tai ohjelmisto-objekti - tyyppinen informaatio, jota voidaan käsitellä sähköisessä muodossa.

Edelleen keksinnön tarkoituksena on tuoda esiin yksinkertainen ja helposti nykytekniikkaan implementoitavissa oleva menetelmä kaupallisten transaktioiden, kuten laskun maksamisen ja pankkiasioinnin, toteuttamiseksi matkaviestimellä.

KEKSINNÖN KOHDE

Keksinnön kohteena on menetelmä sähköisessä muodossa olevan lomakkeen, joka määriteltiin yllä, digitaaliseksi allekirjoittamiseksi turvallisesti käyttäen matkaviestintä tai muuta vastaavaa ja siihen verrattavissa olevaa laitetta. Menetelmässä siirretään allekirjoitettava aineisto, joka voi käsittää ainakin lomakkeen, sen tunnisteen, jaetun datan, ja/tai lomakkeeseen lisätyt olennaiset tiedot, matkaviestimeen. Allekirjoitettava aineisto voidaan muodostaa myös lomakkeen tunnisteesta ja lomakkeeseen liittyvistä olennaisista tiedoista, esimerkiksi lomakkeen ollessa pankkisiirtolomake, voidaan aineisto muodostaa pankkisiirtolomakkeen tunnisteesta ja lomakkeen olennaisten kenttien tiedoista, kuten maksajasta, saajasta ja summasta.

Keksinnön mukaisesti lasketaan allekirjoitettavasta aineistosta ensimmäinen tiiviste edullisesti ennen aineiston siirtämistä matkaviestimeen. Tiiviste lisätään aineistoon siirrettäväksi, jolloin sitä voidaan käyttää apuna tarkistuksen suorittamisessa. Kun aineisto on siirretty matkaviestimeen, se allekirjoitetaan matkaviestimessä ja edelleen keksinnön mukaisesti allekirjoitetun ja siirretyn aineiston oikeellisuus ja vastaavuus varmistetaan vertaamalla allekirjoitettua tiivistettä ja aineistosta ennen allekirjoitusta laskettua tiivistettä keskenään. Allekirjoittaminen voidaan tehdä myös siten, että allekirjoitetaan sekä olennaiset tiedot ja tiiviste, jolloin varmistutaan vielä siitäkin, että matkaviestimellä allekirjoitettu aineisto vastaa allekirjoitettavaksi siirrettyä aineistoa.

Kun kysymyksessä on tietyn tyyppiset sovellukset, kuten maksusovellukset, voidaan matkaviestimeen siirretty aineisto siirtää myös toiselle osapuolelle, esimerkiksi pankille, joka voi laskea saamas-

taan aineistosta tiivisteen. Matkaviestimessä allekirjoitettu aineisto voidaan edelleen salata ja siirtää salattu ja allekirjoitettu aineisto matkaviestimestä myös toiselle osapuolelle. Toinen osapuoli purkaa salauksen, tarkistaa allekirjoituksen, laskee matkaviestimestä saamastaan aineistosta toisen tiivisteen ja vertaa tätä ensimmäiseen alkuperäisestä aineistosta laskemaansa tiivisteeseen. Jos toinen osapuoli hyväksyy digitaalisen allekirjoituksen ja jos ensimmäinen ja toinen tiiviste vastaavat toisiaan, pankki hyväksyy matkaviestimellä tehdyn allekirjoituksen. Kun pankki on hyväksynyt allekirjoituksen, se voi merkitä allekirjoitettuun ja purettuun aineistoon aikaleiman ja arkistoida aineiston allekirjoitustapahtuman.

Edellä on kuvattu menettely, jossa asiakas allekirjoittaa pankille pankilta saamansa lomakkeen. Asiakas tai matkaviestimen käyttäjä voi olla yhteydessä paikallisesti maksuautomaattiin tai vastaavaan, jolloin maksuautomaatti välittää asiakkaalle maksettavaksi ja hyväksyttäväksi tarkoitetun lomakkeen. Tällöin asiakas käy sanomavaihtoa maksuautomaatin kanssa paikallisesti ja maksuautomaatti välittää digitaaliset allekirjoitustiedot edelleen. Kuitenkin maksuautomaatti voi välittämästään liikenteestä päätellä asiakkaan hyväksyneen sille tarjotun palvelun ja maksulomakkeen. Tällöin automaatti voi palvella asiakasta tämän haluamalla ja maksamalla tavalla paikallisesti odottamatta välttämättä pankilta hyväksyntää siitä. Tilanne vastaa käytännössä normaalia käytäntöä, jossa esimerkiksi kaupan kassalla asiakas pankkikortillaan maksaa tuotteet tai palvelut, ja kauppa tarjoaa ne asiakkaalle varmistamatta maksun oikeellisuutta pankista.

Aineisto voidaan myös salata ennen sen siirtämistä matkaviestimeen, jolloin matkaviestimessä on purettava salaus ennen aineiston allekirjoittamista. Tällä voidaan varmistaa se, että vain haluttu matka-

viestin vastaanottaa siirrettävän aineiston ja taata tietojen turvallisuus.

Lomakkeen muodostamiseen voidaan käyttää ennalta sovittua tunnisteellista lomakepohjaa, viestirakennetta tai mitä tahansa muuta sanomarakennetta, johon täydennetään ennalta sovitut oleelliset tiedot ennen lomakkeen siirtämistä matkaviestimeen. Tiiviste voidaan laskea esimerkiksi hash-funktiolla. Viestin ja/tai lomakkeen allekirjoitukseen ja/tai salaukseen voidaan käyttää julkisen ja salaisen avaimen menetelmää.

Keksinnön eräässä edullisessa sovelluksessa esitetään aineisto ja/tai osa siitä matkaviestimessä ennen aineiston allekirjoittamista. Esimerkiksi voidaan esittää lomakkeessa olevat saaja-, maksaja- ja viitetiedot sekä maksettava summa. Myös on mahdollista vaatia matkaviestimen käynnistämistä allekirjoitusmoodissa ennen aineiston siirtämistä siihen. Tämä voi käytännössä tarkoittaa sitä, että matkaviestimeen on syötettävä toinen ennalta määrätty PIN-koodi, jolla matkaviestin on konfiguroitu käynnistymään ennalta määrätyssä allekirjoitusmoodissa. Voidaan käyttää siis eräänlaista paikallista autentikointia.

Keksinnön kohteena on myös järjestelmä sähköisessä muodossa olevan lomakkeen digitaaliseksi allekirjoittamiseksi turvallisesti matkaviestimellä. Järjestelmään kuuluu edullisesti maksuautomaatti ja siihen yhdistetyt välineet allekirjoitettavan aineiston, joka määriteltiin yllä, muodostamiseksi ja siirtämiseksi matkaviestimeen. Maksuautomaatilla voidaan tässä tarkoittaa mitä tahansa paikallista ja paikallisesti käytettävää automaattia, joka voi olla tietoliikenneverkon välityksellä yhdistetty palvelutarjoajaan, kuten pankkiin, kauppaan tai vastaavaan.

Maksuautomaatti voi olla toteutettu myös paikallisesti tietokoneeseen, joka on yhteydessä esimerkiksi Internet-verkon välityksellä palveluntarjoajaan,

jolloin palveluntarjoaja tarjoaa tuotteitaan ja palveluitaan Internet-verkon välityksellä. Tässä tapauksessa allekirjoitettava aineisto siirretään tietokoneelta allekirjoitettavaksi matkaviestimeen paikallista yhteyttä käyttäen tai suoraan palveluntarjoajan omalta palvelimelta käyttämättä paikallista tietokonetta ja yhteyttä.

Keksinnön mukaisesti maksuautomaattiin kuuluu välineet ensimmäisen tiivisteen laskemiseksi allekirjoitettavasta aineistosta. Samaten matkaviestimeen kuuluu allekirjoitusvälineet siihen siirretyn aineiston allekirjoittamiseksi. Allekirjoitusvälineisiin voi kuulua muisti, johon on tallennettu allekirjoituksen ja salauksen vaatimat algoritmit ja avaimet, ja prosessori, joka on yhdistetty muistiin ja joka käsittelee aineistoa toteuttaen digitaalisen allekirjoituksen ja mahdollisesti salauksen. Lisäksi maksuautomaattiin kuuluu välineet allekirjoitetun ja siirretyn aineiston oikeellisuuden varmistamiseksi vertaamalla matkaviestimessä allekirjoitettua tiivistettä ja aineistosta ennen allekirjoitusta laskettua tiivistettä keskenään.

Järjestelmään voi myös kuulua palvelin, joka on yhdistetty maksuautomaattiin ja/tai matkaviestimeen ja joka on toisen osapuolen, kuten pankin tai luottokorttiyhtiön, valvonnassa. Tällainen palvelin voi siis olla esimerkiksi pankin ylläpitämä ja sitä voidaan käyttää pankkitapahtumien toteuttamisessa. Palvelimeen voi myös kuulua välineet matkaviestimen tekemän digitaalisen allekirjoituksen oikeellisuuden todentamiseksi ja salaus- ja purkuvälineet palvelimen ja maksuautomaatin ja/tai matkaviestimen välillä siirrettävän aineiston salaamiseksi ja purkamiseksi.

Palvelimeen voi kuulua myös välineet aikaleiman merkitsemiseksi aineistoon ja välineet aineiston allekirjoitustapahtuman arkistoimiseksi sen jälkeen, kun allekirjoitus on todettu oikeaksi. Nämä voi-

daan toteuttaa ammattimiehen sinänsä tuntemalla tavalla, eikä niitä sen vuoksi kuvata tässä tarkemmin.

Esillä olevan keksinnön etuna tunnettuun tekniikkaan verrattuna on, että keksinnön ansiosta maksusovellusten, varmistustapahtumien ja muiden toteuttaminen matkaviestimellä tulee entistä helpommaksi. Keksinnön ansiosta matkaviestintä voidaan luotettavasti käyttää digitaalisessa allekirjoituksessa ja tällöin digitaalinen allekirjoitus voidaan yhdistää monen eri sovelluksen yhteyteen.

KUVALUETTELO

Seuraavassa keksintöä selostetaan edullisten sovellusesimerkkien avulla viittaamalla oheiseen piirustukseen, jossa:

kuvio 1 esittää erästä esillä olevan keksinnön mukaista edullista järjestelmää;

kuvio 2 esittää erästä toista esillä olevan keksinnön mukaista edullista järjestelmää;

kuvio 3 esittää vuokaaviomuodossa esillä olevan keksinnön erään edullisen sovelluksen; ja

kuvio 4 esittää kaaviomaisesti erään edullisen esimerkin allekirjoitettavan aineiston muodostamisesta esillä olevan keksinnön yhteydessä.

Kuviossa 1 esitettyyn järjestelmään kuuluu paikallinen maksuautomaatti (Local Payment Machine, LPM) 2 ja siihen yhdistetyt välineet allekirjoitettavan aineiston, käsittäen lomakkeen, sen tunnisteen, jaetun datan ja/tai siihen liitetyt olennaiset tiedot, muodostamiseksi. Lisäksi maksuautomaattiin kuuluu siihen yhdistetyt välineet 4 aineiston siirtämiseksi matkaviestimeen. Vastaavasti matkaviestimeen kuuluu välineet 1, joilla matkaviestin (MS) kommunikoi maksuautomaatin kanssa. Eräässä edullisessa sovelluksessa välineet 1 ja 4 on toteutettu Bluetooth-teknologiaa käyttäen. Tarkempaa kuvausta Bluetooth-tekniikasta esitetään esimerkiksi WWW-sivulla www.bluetooth.com. Myös

muita tunnettuja siirtoyhteyskäytäntöjä, kuten infrapunaliitäntää voidaan käyttää

Edelleen kuviossa 1 esitettyyn järjestelmään kuuluu palvelin 8, joka on yhdistetty TCP/IP-yhteydellä maksuautomaattiin 2 ja joka tässä esimerkissä on pankin hallinnoima. Palvelimeen kuuluu edelleen välineet 9 digitaalisen allekirjoituksen oikeellisuuden todentamiseksi - käytännössä niillä puretaan vastaanotetut salaviestit ja verrataan niissä olevia digitaalisia allekirjoituksia saatuihin käyttäjätietoihin. Lisäksi palvelimeen kuuluu välineet 11 ja 12, joilla merkitään aikaleima allekirjoitettuun aineistoon ja arkistoidaan allekirjoitustapahtuma sen jälkeen, kun allekirjoitus on todettu oikeaksi. Vastaavat todentamisvälineet voivat kuulua myös maksuautomaattiin ja tässä ne on merkitty numerolla 7. Välineillä 7, 11 ja 12 voi olla myös ominaisuus, jolla tarvittavat julkiset avaimet noudetaan esimerkiksi TCP/IP-verkon välityksellä yleisiltä avainhallintapalvelimilta.

Kuvion 1 esimerkissä siirretään salattu aineisto, johon kuuluu laskulomake ja laskulomakkeesta laskettu tiiviste H1 maksuautomaatilta 2 matkaviestimeen MS, vaihe 1. Matkaviestimessä aineisto eli laskulomake ja siihen tallennetut tiedot maksun saajasta, maksajasta, summasta ja maksun viitteestä esitetään matkapuhelimen näytöllä (10), josta matkaviestimen käyttäjä voi tarkistaa, mitä on allekirjoittamassa. Sen jälkeen käyttäjä allekirjoittaa matkaviestimellä MS aineiston ja siitä lasketun tiivisteen H1. Aineisto, johon on lisätty tiiviste $H1_{ds}$ allekirjoitettuna digitaalisesti siirretään maksuautomaattiin 2, vaihe 2. Maksuautomaatin 2 ja matkaviestimen MS välinen sanomaliikenne voidaan salata käyttäen matkaviestimen käyttäjän ja maksuautomaatin julkisia ja salaisia avaimia. Kun maksuautomaatissa 2 on tarkistettu allekirjoituksen oikeellisuus, lähetetään clearing-sanoma,

vaihe 3 maksuautomaatista edelleen pankkiin. Clearing on tunnettua ja yleisesti pankkimaailmassa käytettyä tekniikkaa eikä sitä kuvata tässä tarkemmin.

Seuraavaksi viitataan kuvioon 2, jossa on esitetty vastaavanlainen järjestelmä kuin kuviossa 1, mutta tässä järjestelmää käytetään hieman eri tavalla. Ensin maksuautomaatissa muodostettu aineisto, esimerkiksi lomake, siirretään pankkiin, vaihe 1. Sen jälkeen aineistosta lasketaan maksuautomaatissa tiiviste H1, joka siirretään matkaviestimeen allekirjoitettavaksi, vaihe 2. Siirto voidaan tehdä käyttäen paikallista esimerkiksi Bluetooth-yhteyttä. Matkaviestimessä saatu sanoma allekirjoitetaan digitaalisesti ja sen jälkeen allekirjoitettu ja mahdollisesti salattu aineisto lähetetään pankkiin, vaihe 3. Pankissa verrataan maksuautomaatilta saadusta aineistosta laskettua tiivistettä H1 matkaviestimeltä saatuun tiivisteeseen $H1_{ds}$, joka on digitaalisesti allekirjoitettu ja jos ne täsmäävät, hyväksytään allekirjoitustapahtuma. Tämän jälkeen palvelimella tehdään aikaleimaus ja arkistoidaan saatu allekirjoitustapahtuma. Pankki voi olla myös muu vastaava palveluntarjoaja, kuten luottokorttiyhtiö, jolloin edellä kuvatun lisäksi allekirjoituksen oikeellisuus vahvistetaan pankille, maksuautomaatille tai muulle palveluntarjoajalle. Tällöin luottokorttiyhtiö vahvistettuaan allekirjoituksen ottaa vastuun tapahtumasta.

Viitaten vielä kuvioon 3 esitetään eräs keksinnön edullinen sovellus. Aluksi muodostetaan aineisto, joka on tarkoitettu allekirjoitettavaksi matkaviestimellä, lohko 31. Aineistosta lasketaan ensimmäinen tiiviste, H1, lohko 32. Sen jälkeen tarkistetaan, lohko 45, onko aineisto salattava ennen lähetystä matkaviestimeen. Jos aineisto on salattava, siirrytään lohkoon 46 ja salataan se käyttäen matkaviestimen käyttäjän julkista avainta. Salauksen jälkeen siirrytään lohkoon 33. Jos aineistoa ei tarvitse salata,

siirrytään suoraan lohkoon 33, jossa aineisto siirretään matkaviestimelle. Seuraavaksi siirrytään lohkoon 34 ja tarkistetaan matkaviestimen näytöllä esitettävä aineisto tai sen olennaiset tiedot eli esimerkiksi laskun saajan ja maksun oikeellisuus. Jos maksaja hyväksyy, lohkossa 35, siirrytään lohkoon 37 ja allekirjoitetaan aineisto. Jos maksaja ei hyväksy lohkossa 35, siirrytään lohkoon 36, jossa lähetetään hylkäyssanoma aineiston lähettäjälle, esimerkiksi maksuautomaatille ja lopetetaan prosessi. Lohkosta 37 siirrytään lohkoon 38, jossa muodostetaan aineisto digitaalisesta allekirjoituksesta ja tiivisteestä ja mahdollisesti saadusta aineistosta, johon kuuluu esimerkiksi lomakkeen olennaiset tiedot, lohko 38. Sen jälkeen aineisto siirretään maksuautomaattiin, lohko 39, josta edelleen siirrytään lohkoon 40 ja verrataan siirretystä aineistosta laskettua tiivistettä allekirjoitettuun tiivisteeseen. Jos tiivisteet vastaavat toisiaan, lohko 41, hyväksytään allekirjoitus ja tehdään seuraavaksi määritellyt toimenpiteet.

Jos lohkossa 40 tiivisteet eivät täsmänneet, voidaan proseduuri toistaa. Tässä vaiheessa on mahdollista käyttää laskuria, jolla tarkkaillaan sitä, ettei aineistoa lähetetä useammin kuin ennalta on sovittu. Lohkosta 40 siirrytään lohkoon 43, jossa kasvatetaan laskurin k = k+1 arvoa yhdellä ja siitä edelleen siirrytään lohkoon 44, jossa tarkistetaan laskurin arvo eli se, montako kertaa aineisto on siirretty matkaviestimeen. Jos arvo ylittää ennalta sovitun, siirrytään lohkoon 42 ja lähetetään hylkäyssanoma matkaviestimeen. Jos laskurin arvo on pienempi kuin ennalta sovittu, siirrytään uudelleen lohkoon 31 ja toistetaan prosessi.

Kuviossa 4 on esitetty eräs edullinen tapa muodostaa ja allekirjoittaa lomake tai aineisto digitaalisesti. Matkaviestimeen siirrettävään aineistoon kuuluu lomaketunniste, joka on yksilöllinen kaikille

käytettäville lomakkeille, lohko 51. Lomaketunnisteeseen liittyy lomakekaavain, lohko 52, joiden perusteella sovellukset, asiakas ja sovelluksen tarjoaja tietävät tarkalleen, millaisesta lomakkeesta on kysymys. Aineistoa muodostettaessa lomaketunniste ja lomakekaavain ketjutetaan peräkkäin, kuten kuviossa 4 on esitetty ja sen jälkeen niistä lasketaan ensimmäinen tiiviste, lohko 54.

Lomakkeeseen liitetään usein lomakedataa, lohko 53, jo ennen sen siirtämiseksi matkaviestimeen allekirjoitettavaksi. Tällöin lomaketunniste ja lomakedata ketjutetaan peräkkäin kuvion 4 osoittamassa järjestyksessä ja niistä saatu bittijono edelleen ketjutetaan satunnaisten 16 tavun, lohko 55 kanssa. Niihin yhdistetään ensimmäinen tiiviste lohkosta 54.

Tässä vaiheessa aineisto on valmis siirrettäväksi matkaviestimeen, minkä jälkeen siitä lasketaan toinen tiiviste, lohko 56. Käytännössä toinen tiiviste lasketaan matkaviestimessä ja lisätään allekirjoitettavaan sanomaan, lohko 57. Samaten allekirjoitettavaan sanomaan on lisätty käyttäjädata, jota matkaviestimen käyttäjä on voinut täydentää omilla tiedoillaan tarpeen mukaan. Edullisesti myös tähän allekirjoitettavaan viestiin lisätään lohkosta 55 16 satunnaistavua, jolloin aineiston siirtäjän ja matkaviestimen käyttäjän muodostaman allekirjoitetun sanoman oikeellisuutta voidaan tarkistaa. Kun satunnaistavut käyttäjädata ja toinen tiiviste on asetettu peräkkäin, käyttäjän matkaviestimessä allekirjoitetaan sanoma digitaalisesti. Tämän jälkeen sanoma voidaan välittää eteenpäin toiselle osapuolelle, maksuautomaattiin tai muulle aineiston alkuperälähteelle.

Yhteenvetona todetaan vielä, että keksintönä on toteuttaa menetelmä ja järjestelmä, jossa käyttäjä, palvelun tarjoaja ja pankki, jotka mainitaan esimerkkinä, voivat varmistua digitaalisen allekirjoituksen oikeellisuudesta. Tarkoituksena on, että allekirjoi-

tettava aineisto voidaan sitoa johonkin käyttäjän dataan, formaattiin ja käyttäjän tekemään digitaaliseen allekirjoitukseen. Allekirjoitus on siis pystyttävä sitomaan tietynlaiseen ketjuun, joka käytännössä vastaa nykyisin käytössä olevaa ketjua, jossa käyttäjä omalla manuaalisella allekirjoituksellaan hyväksyy ostoksiaan. Samaten menetelmän tarkoituksena on identifioida allekirjoittaja luotettavasti ja lainsäätäjän vaatimalla ja tarkoittamalla tavalla.

Esillä olevaa keksintöä ei rajata tässä esitettyihin esimerkkeihin, vaan monet muunnokset ovat mahdollisia pysyttäessä oheisten patenttivaatimusten määrittelemän suojapiirin rajoissa.

PATENTTIVAATIMUKSET

1. Menetelmä sähköisessä muodossa olevan lomakkeen digitaaliseksi allekirjoittamiseksi turvallisesti matkaviestimellä, johon menetelmään kuuluu vaiheet

siirretään allekirjoitettava aineisto, johon kuuluu lomake, sen tunniste, jaettu data, ja/tai siihen lisätyt olennaiset tiedot, matkaviestimeen, t u n n e t t u siitä, että

lasketaan allekirjoitettavasta aineistosta ensimmäinen tiiviste (H1);

lisätään tiiviste aineistoon siirrettäväksi matkaviestimeen;

allekirjoitetaan digitaalisesti matkaviestimellä siihen siirretty aineisto; ja

varmistetaan allekirjoitetun ja siirretyn aineiston oikeellisuus vertaamalla allekirjoitettua tiivistettä ja aineistosta ennen allekirjoitusta laskettua tiivistettä keskenään.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että

siirretään matkaviestimeen allekirjoitettavaksi siirretty aineisto toiselle osapuolelle; ja

allekirjoitettu aineisto toiselle osapuolelle, jolloin toinen osapuoli varmistaa allekirjoituksen oikeellisuuden.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että salataan aineisto ennen sen siirtämistä matkaviestimen ja toisen osapuolen välillä; ja

puretaan salaus ennen aineiston käsittelyä, kuten allekirjoitusta ja oikeellisuuden varmistamista.

4. Jonkin edeltävistä patenttivaatimuksista 1 - 3 mukainen menetelmä, t u n n e t t u siitä, että

käytetään lomakkeen muodostamiseen ennalta sovittua tunnisteellista lomakepohjaa, johon täydennetään

oleelliset tiedot ennen sen siirtämistä matkaviestimeen.

5. Jonkin edeltävistä patenttivaatimuksista 1 - 4 mukainen menetelmä, t u n n e t t u siitä, että

muodostetaan tiiviste hash-funktiolla.

6. Jonkin edeltävistä patenttivaatimuksista 1 - 5 mukainen menetelmä, t u n n e t t u siitä, että

käytetään viestin allekirjoitukseen ja/tai salaukseen julkisen ja salaisen avaimen menetelmää.

7. Jonkin edeltävistä patenttivaatimuksista 1 - 6 mukainen menetelmä, t u n n e t t u siitä, että

esitetään aineisto ja/tai osa siitä matkaviestimessä ennen aineiston allekirjoittamista.

8. Jonkin edeltävistä patenttivaatimuksista 1 - 7 mukainen menetelmä, t u n n e t t u siitä, että

käynnistetään matkaviestin allekirjoitusmoodissa ennen aineiston siirtämistä matkaviestimeen.

9. Jonkin edeltävistä patenttivaatimuksista 1 - 8 mukainen menetelmä, t u n n e t t u siitä, että

merkitään aineistoon aikaleima; ja

arkistoidaan aineiston allekirjoitustapahtuma sen jälkeen, kun allekirjoitus on todettu oikeaksi.

10. Järjestelmä sähköisessä muodossa olevan lomakkeen digitaaliseksi allekirjoittamiseksi turvallisesti matkaviestimellä (MS), johon järjestelmään kuuluu

maksuautomaatti (2);

maksuautomaattiin yhdistetyt välineet (3) allekirjoitettavan aineiston, johon kuuluu lomake, sen tunniste, jaettu data, ja/tai siihen lisätyt olennaiset tiedot, muodostamiseksi; ja

maksuautomaattiin yhdistetyt välineet (4) aineiston siirtämiseksi matkaviestimeen (MS), t u n n e t t u siitä, että

maksuautomaattiin kuuluu välineet (5) ensimmäisen tiivisteen (H1) laskemiseksi allekirjoitettavasta aineistosta;

matkaviestimeen kuuluu allekirjoitusvälineet (6) siihen siirretyn aineiston allekirjoittamiseksi; ja

maksuautomaattiin kuuluu välineet (7) allekirjoitetun ja siirretyn aineiston oikeellisuuden varmistamiseksi vertaamalla allekirjoitettua tiivistettä ($H1_{ds}$) ja aineistosta ennen allekirjoitusta laskettua tiivistettä (H1) keskenään.

11. Patenttivaatimuksen 10 mukainen järjestelmä, t u n n e t t u siitä, että järjestelmään kuuluu

palvelin (8), joka on yhdistetty maksuautomaattiin (2) ja matkaviestimeen (MS) ja kolmannen osapuolen valvonnassa; ja

matkaviestimeen kuuluu välineet allekirjoitetun aineiston salaamiseksi.

12. Patenttivaatimuksen 10 tai 11 mukainen järjestelmä, t u n n e t t u siitä, että palvelimeen (8) kuuluu

välineet (9) digitaalisen allekirjoituksen oikeellisuuden todentamiseksi.

13. Jonkin edeltävistä patenttivaatimuksista 10 - 12 mukainen menetelmä, t u n n e t t u siitä, että matkaviestimeen kuuluu

välineet (10) aineiston ja/tai osan siitä esittämiseksi matkaviestimessä ennen aineiston allekirjoittamista.

14. Jonkin edeltävistä patenttivaatimuksista 10 - 13 mukainen menetelmä, t u n n e t t u siitä, että palvelimeen (8) kuuluu

välineet (11) aikaleiman merkitsemiseksi aineistoon; ja

välineet (12) aineiston allekirjoitustapahtuman arkistoimiseksi sen jälkeen, kun allekirjoitus on todettu oikeaksi.

(57) TIIVISTELMÄ

Menetelmä sähköisessä muodossa olevan lomakkeen digitaaliseksi allekirjoittamiseksi turvallisesti matkaviestimellä. Menetelmässä siirretään allekirjoitettava aineisto, johon kuuluu lomake, sen tunniste, jaettu data, ja/tai siihen lisätyt olennaiset tiedot, matkaviestimeen, lasketaan allekirjoitettavasta aineistosta ensimmäinen tiiviste (H1), lisätään tiiviste aineistoon siirrettäväksi matkaviestimeen, allekirjoitetaan digitaalisesti matkaviestimellä siihen siirretty aineisto ja varmistetaan allekirjoitetun ja siirretyn aineiston oikeellisuus vertaamalla allekirjoitettua tiivistettä ja aineistosta ennen allekirjoitusta laskettua tiivistettä keskenään. Keksinnön ansiosta matkaviestintä voidaan turvallisesti käyttää digitaaliseen allekirjoitukseen erilaisissa sovelluksissa.

(Fig. 1)

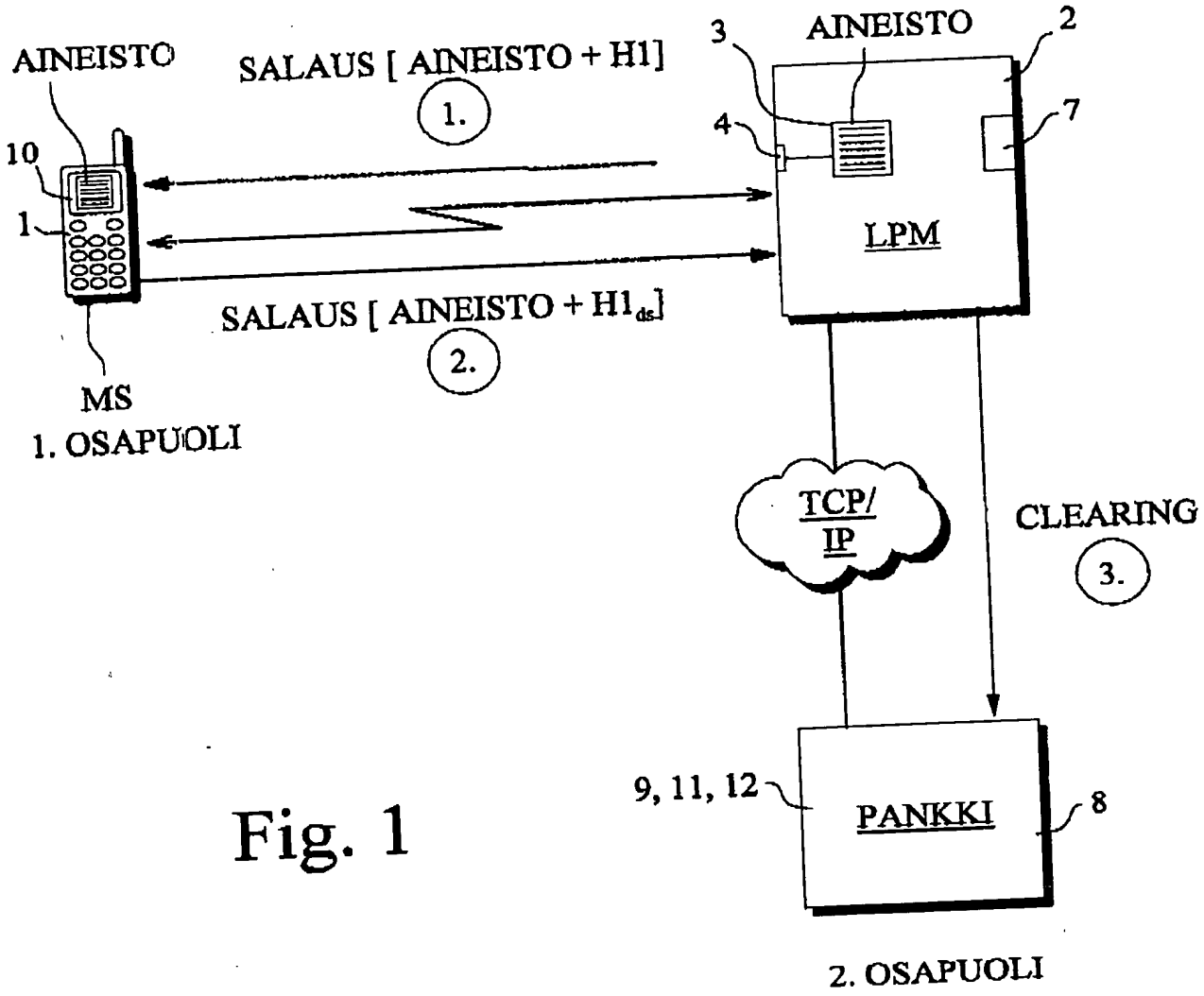
AINEISTO
SALAUS [AINEISTO + H1]
1.
3
AINEISTO
2
4
7
10
1
LPM
SALAUS [AINEISTO + H1ds]
2.
MS
1. OSAPUOLI
TCP/
IP
CLEARING
3.
9, 11, 12
PANKKI
8
2. OSAPUOLI

Fig. 1

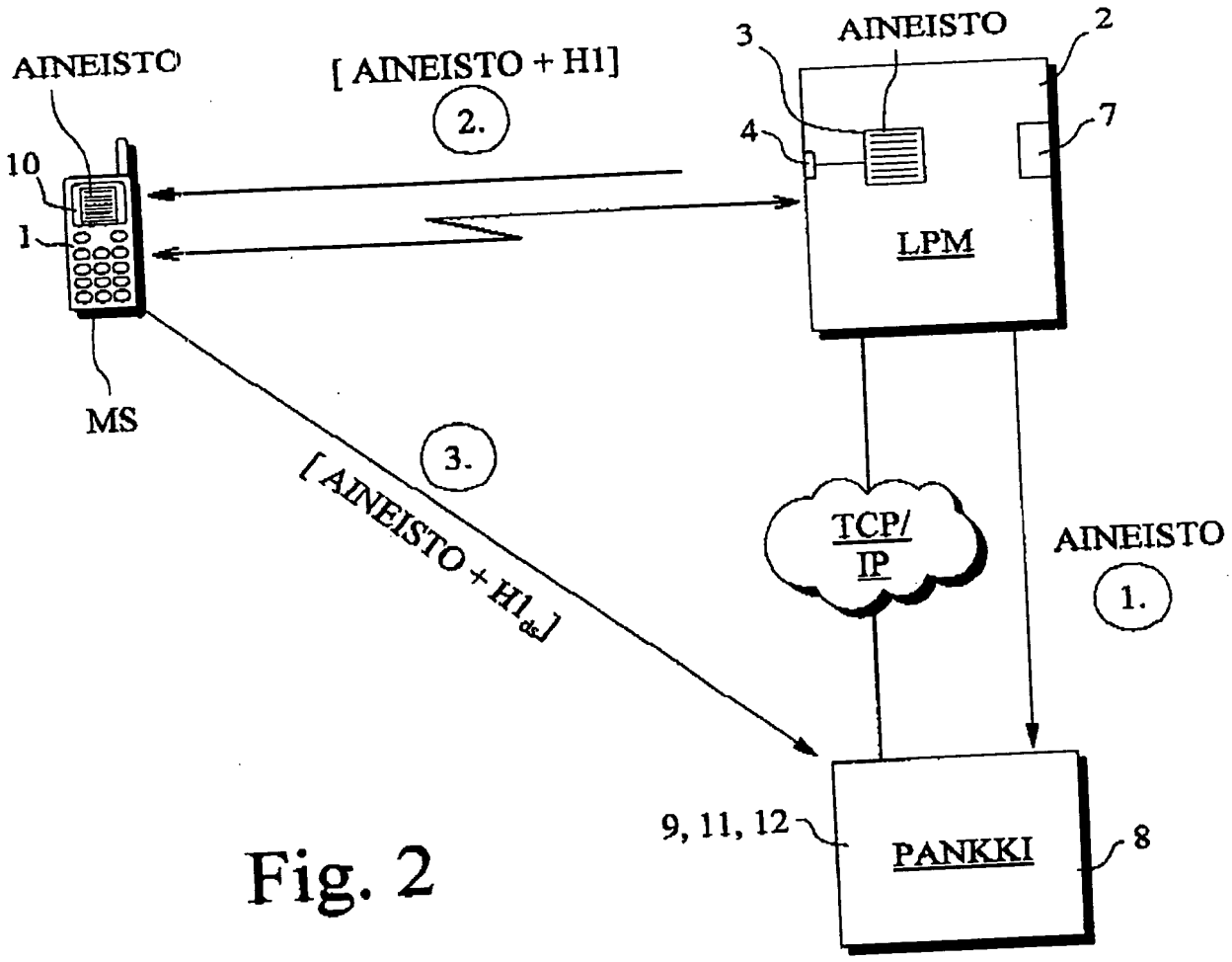
AINEISTO
[AINEISTO + H1]
2.
3
AINEISTO
2
4
7
10
1
LPM
MS
3.
[AINEISTO + H1$_{dd}$]
TCP/
IP
AINEISTO
1.
9, 11, 12
PANKKI
8

Fig. 2

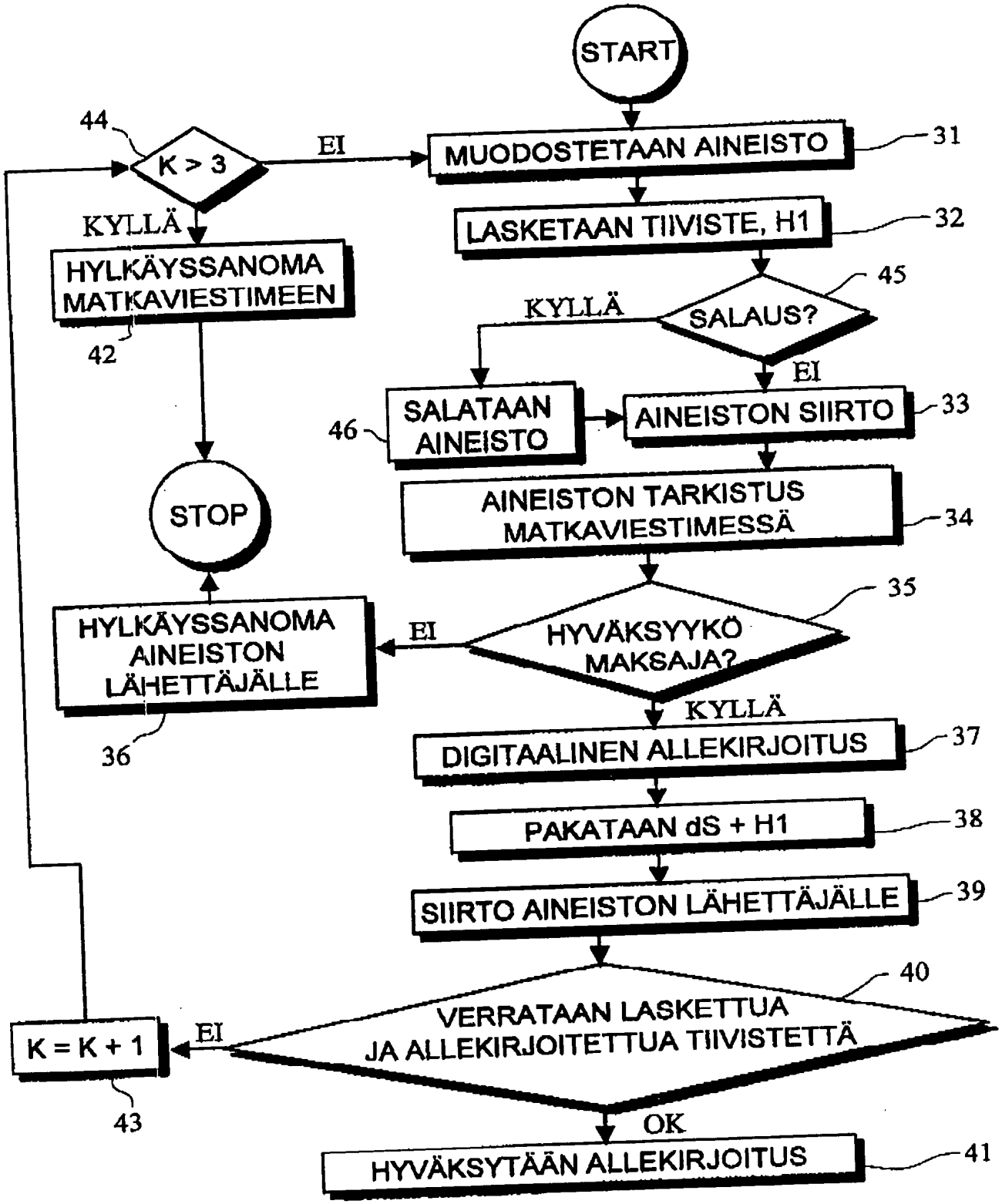
START
MUODOSTETAAN AINEISTO
31
LASKETAAN TIIVISTE, H1
32
SALAUS?
45
KYLLÄ
EI
SALATAAN AINEISTO
46
AINEISTON SIIRTO
33
AINEISTON TARKISTUS MATKAVIESTIMESSÄ
34
HYVÄKSYYKÖ MAKSAJA?
35
EI
KYLLÄ
HYLKÄYSSANOMA AINEISTON LÄHETTÄJÄLLE
36
DIGITAALINEN ALLEKIRJOITUS
37
PAKATAAN dS + H1
38
SIIRTO AINEISTON LÄHETTÄJÄLLE
39
VERRATAAN LASKETTUA JA ALLEKIRJOITETTUA TIIVISTETTÄ
40
EI
OK
K = K + 1
43
HYVÄKSYTÄÄN ALLEKIRJOITUS
41
K > 3
44
EI
KYLLÄ
HYLKÄYSSANOMA MATKAVIESTIMEEN
42
STOP

Fig. 3

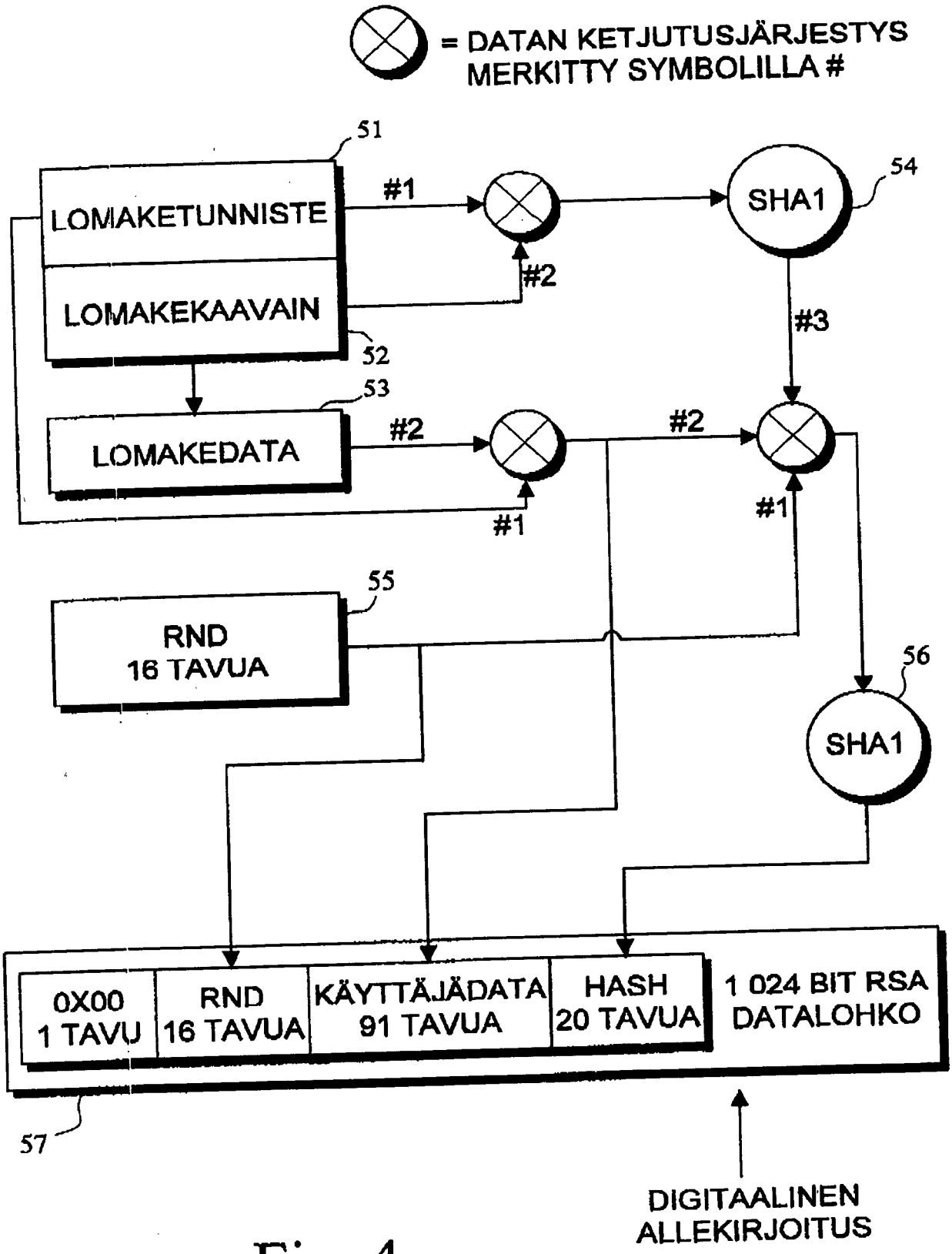
= DATAN KETJUTUSJÄRJESTYS MERKITTY SYMBOLILLA #
51
LOMAKETUNNISTE
LOMAKEKAAVAIN
52
#1
#2
SHA1
54
#3
53
LOMAKEDATA
#2
#2
#1
#1
55
RND
16 TAVUA
56
SHA1
0X00
1 TAVU
RND
16 TAVUA
KÄYTTÄJÄDATA
91 TAVUA
HASH
20 TAVUA
1 024 BIT RSA
DATALOHKO
57
DIGITAALINEN
ALLEKIRJOITUS

Fig. 4

This Page Blank (uspto)